Operational Resilience

Managing, Protecting, and Sustaining Organizational Missions

Dr. Nader Mehravari, MBCP, MBCI

CERT Resilience Management Team
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/resilience/

January 23, 2014

Report Documentation Page			Form Approved OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **23 JAN 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Operational Resilience: Managing, Protecting, and Sustaining Organizational Missions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Mehravari /Nader	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon Software Engineering Institute, 4500 Fifth Ave, Pittsburgh, PA 15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited.**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **72**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Notices

Contents

Organizational Mission

- Setting the Stage

Operational Stress

- Disruptive Events

Yesterday vs. Today

- Expansion of Risk Environment

Operational Resilience

- Operational Risk & Mission Success

Organizational Mission – Revisited

- Approach for Resilience Management, Protection, and Sustainment

Success Stories

- A Sampling of Real-Life Applications

Closing

Organizational Mission

"The American Red Cross prevents and alleviates human suffering in the face of emergencies by mobilizing the power of volunteers and the generosity of donors."

Disaster Relief	Safe and Adequate Blood Supply	Health and Safety Education

"To provide postal services to bind the Nation together … To provide prompt, reliable, and efficient services to patrons in all areas and … render postal services to all communities."

Delivering Mail	Selling Stamps	Ensuring Mail Safety	Operating a 37,000-node intranet

"Provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations."

DISN, NIPRNET, SIPRNET…	Enterprise Email Services	Spectrum	Tactical InfoSec Services	

Contributing positively to the earth's natural ecosystem.

| Shade | Habitat for Birds | Climbing Opportunity | Beauty | • • • |

Operational Stress

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home ▾ | CFO Journal   CIO Journal   Today's Paper   Video   Blogs   Journal Comm

World ▾ | U.S. ▾ | New York ▾ | **Business ▾** | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life &

Small Business ▾

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketin

BUSINESS | Updated April 16, 2012, 8:21 p.m. ET

Tornadoes Hamper Boeing Supplier

*Spirit Says Output Suspended 'At Least' Through Tuesday, Deliveries Could Res
of Week*

| **Article** | **Stock Quotes** | **Comments** |

By JON OSTROWER

WICHITA, Kan.—A key Boeing Co. [BA +2.51%] supplier said it aims to res
deliveries by the end of the week after tornadoes battered its factories here
highlighting the fragility and resilience of the aerospace giant's global supp
it works to sharply increase production.

The storms late Saturday caused significant-to-major damage to 10 buildi
flagship campus of Spirit AeroSystems Inc., which makes fuselages and c
for Boeing's hot-selling 737, 777 and 787 Dreamliner passenger jets. Spirit
said production—which normally runs seven days a week—would be susp
least" through Tuesday, and that it expects "near-term production disrupti
including delivery impacts" to customers.

Spirit spokesman Ken Evans
assessments found most of it
machinery and inventory intact. "We
believe we can use the facilities we've
got," he said in an interview here in
Wichita, a major manufacturing hub for
the aerospace industry. "We don't

Software Engineering Institute | Carnegie Mellon University

THE WALL STREET JOURNAL.
PROFESSIONAL WITH FACTIVA

U.S. Edition Home ▾ | CFO Journal   CIO Journal   Today's Paper   Video   Blogs   Journal Commu

World ▾ | U.S. ▾ | New York ▾ | **Business** ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life
Small Business ▾

Asia | Europe | Earnings | Economy | Health | Law | **Autos** | Management | Media & Marketing

AUTOS | Updated April 17, 2012, 8:36 p.m. ET

Nylon-12 Haunts Car Makers

Explosion at Big Supplier of Resin for Automotive Parts Has Indu
Shortages

Article | Stock Quotes | Comments (9)

By JEFF BENNETT And JAN HROMADKO

Production shortfalls at a single German auto-parts supplier are beginni
through the global auto business.

More than 200 auto executives met in a Detroit suburb on Tuesday to evaluate a
looming shortage of a relatively obscure resin essential to modern auto production.

Inventories of the resin are being depleted a
Industries AG plant in Marl, Germany, that
itself as the only integrated maker of the re
lines.

production before the winter this year
and expect that the works to fully repair
the plant will take at least three
months," an Evonik spokeswoman said.
Several Evonik executives attended the
meeting on Tuesday.

Chemical plant explosion brakes car makers

The explosion at a German chemicals plant two weeks ago which killed two workers, has thrown the global car industry into turmoil as manufacturers run short of a vital component, prompting an emergency meeting in Detroit.

WHAT 'OBSCURE' BUT ESSENTIAL COMPOUND SHORTAGE HAS THE AUTO INDUSTRY WORRIED ABOUT PRODUCTION?

THE WALL STREET JOURNAL | News Alert

Computer Glitch Halts American Airlines Flights

The Federal Aviation Administration is holding all American Airlines flights at their origin airports until at least 5 p.m. Eastern time on Tuesday while the carrier tries to resolve a nationwide outage to its reservations system.

THE WALL STREET JOURNAL.

U.S. EDITION ▾ Tuesday, April 16, 2013 As of 5:28 PM EDT

Home | World ▾ | U.S. ▾ | New York ▾ | **Business** ▾ | Tech ▾ | Markets ▾ | Market Data | Opinion ▾

BUSINESS | Updated April 16, 2013, 5:28 p.m. ET

Outage Snarls American Air Flights

By JACK NICAS And SUSAN CAREY

SANDY SHUTS DOWN THE CITY

By JOHN ANNESE
and JILLIAN JORGENSEN
STATEN ISLAND ADVANCE

The city is in a virtual lockdown as a storm of unprecedented character slammed into the East Coast,

Tracking the storm

The worst of the powerful hurricane is expected Monday night into Tuesday

Hospital evacuated

THE WALL STREET JOURNAL. ≡ | WORLD
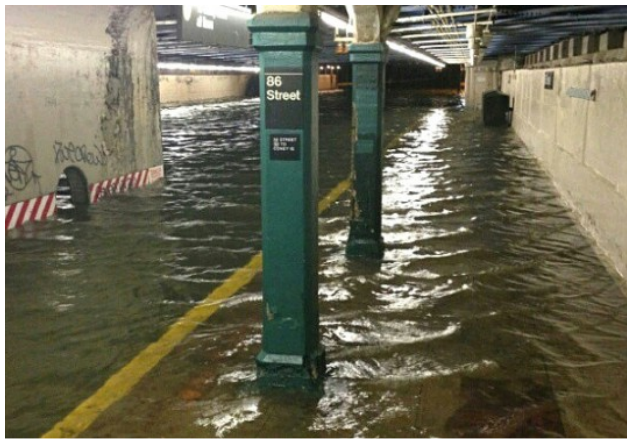
Powerful Typhoon Haiyan Hits Philippines

By CRIS LARANO and JOSEPHINE CUNETA

Nov. 7, 2013 10:44 a.m. ET

Week of 4/22/13

THE WALL STREET JOURNAL. | NEW YORK

April 19, 2013, 1:37 PM

Train Halt From Boston Stretches to Manhattan

TIME
U.S.

Magazine | Video | LIFE | TIME 100

SUBSCRIBE

NEWSFEED | **U.S.** | **POLITICS** | **WORLD** | **BUSINESS** | **TECH** | **HEALTH** | **SCIENCE** | ENTE

NATIONAL

The Marathon Bombing: Gunfights, Blasts and a Manhunt Shut Down Boston

By Jay Newton-Small / Watertown | April 19, 2013 | 0

U.S.NEWS on NBCNEWS.com

Compare hundreds of

Updated
3
days
ago

Boston transit shut down, nearly 1 million sheltering in place amid terror hunt

Article Talk

Advanced persistent threat

From Wikipedia, the free encyclopedia

Advanced persistent threat (APT) usually refers to a group, such as a foreig[n]
effectively target a specific entity. The term is commonly used to refer to cyb[er]
intelligence gathering techniques to access sensitive information[1], but app[lies]
Other recognized attack vectors include infected media, supply chain compro[mise]
usually referred to as an APT as they rarely have the resources to be both adv[anced and persistent at]
a specific target.[3]

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
[Don]ate to Wikipedia
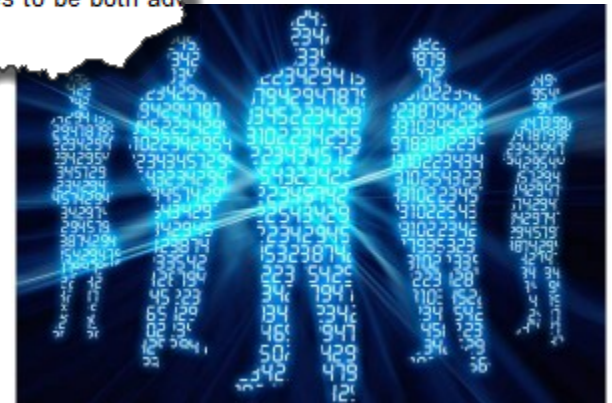
Thursday, January 31, 2013 As of 8:28 PM EST

THE WALL STREET JOURNAL.
PROFESSIONAL WITH FACTIVA

U.S. Edition Home ▾ | CFO Journal   CIO Journal   Today's Paper   Video   Blogs   Journal Community

Home | World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Tech ▾ | Markets ▾ | Market Data | Opinion ▾

MEDIA & MARKETING | Updated January 31, 2013, 8:28 p.m. ET

Chinese Hackers Hit U.S. Media
Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Several Years

By SIOBHAN GORMAN, DEVLIN BARRETT and DANNY YADRON

WASHINGTON—Chinese hackers believed to have government links have been conducting wide-ranging electronic surveillance of media companies including The Wall Street Journal, apparently to spy on reporters covering China and other issues, people familiar with the incidents said.

Journal publisher Dow Jones & Co. said Thursday that the paper's computer systems had been infiltrated by Chinese hackers, apparently to monitor its China coverage.
New York Times Co. [NYT +0.11%] disclosed Wedn...
newspaper also had been the victim of cyberspying...

The Washington Post
Politics | Opinions | Local | Sports | National | World | Business | Tec

More companies reporting cybersecurity incidents

By Ellen Nakashima and Danielle Douglas, Published: March 1

At least 19 financial institutions have disclosed to investors in computers were targets of malicious cyberassaults last year, a among corporations about the breadth of cybersecurity incide sector.

In their annual financia such as Bank of America institutions, have repor intrusions.

THE WALL STREET JOURNAL.
U.S. EDITION ▾ Saturday, March 16, 2013 As of 4:17 PM EDT New York 38°|28°

Home | World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Tech ▾ | Markets ▾ | Market Data | Opinion

DDoS Attacks on U.S. Banks: Worst Yet to Come?
February 19, 2013, 12:01am

gainst U.S. banks last fall
bilities, whereas the intent of
e been to simply cause

Gartner.
WHY GARTNER | ANALYSTS | RESEARCH | EVENTS | CONSULTING | ABOUT

Are the ongoing DDoS attacks against U.S. banks just the calm before the storm?
by Avivah Litan | March 14, 2013 | 1 Comment

That's a viable hypotheses after hearing that the attackers only used one third of the bandwidth they had staged for their latest round of attacks against U.S. banks last Tuesday. Reportedly, on Tuesday the total size of the DDoS attack was 190 gigabits at one time, with the largest attack against a single bank at 110 gigabits.

Interestingly, the attackers could have easily done even more damage but they chose not to. 9200 bots were identified as attack-capable but the total number of bots actually involved in sending the DDoS traffic to the banks numbered only about 3200. The other 6000 bots sat there doing nothing.

April 23, 2013

CSO | SECURITY AND RISK   Newsletters   Dashboard   RSS   Research Centers ▾   White P...

Pacemaker hack can deliver deadly 830-volt jolt

Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination

By Jeremy Kirk

October 17, 2012 — IDG News
a deadly, 830-volt shock from so
medical device companies.

SCIENTIFIC AMERICAN™

Sign In / Register

Search ScientificAmerican.com

Health :: News :: June 25, 2013 :: 💬 5 Comments :: ✉ Email :: 🖶 Print

A New Cyber Concern: Hack Attacks on Medical Devices

THE WALL STREET JOURNAL.

U.S. EDITION ▾ Thursday, June 13, 2013 As of 7:33 PM EDT

Home   World ▾   U.S. ▾   Business ▾   Tech ▾   Markets ▾   Market Data   Your Money ▾   Opinion ▾   Life & C...

U.S. NEWS | June 13, 2013, 7:33 p.m. ET

Patients Put at Risk By Computer Viruses

By CHRISTOPHER WEAVER

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of

Challenges to Organizational Mission

Operational mission of organizations is under stress on a minute-by-minute basis.

The stress comes from

- pervasive use of technology
- globalization
- complexity of business processes
- operational complexity
- movement toward intangible assets
- global economic pressures
- open borders
- geo-political pressures
- regulatory and legal boundaries
- intertwining of cyber and physical domains
- terrorists & professional hackers

…and is exasperated by increased intertwining of cyber and physical domains.

Disruptive Events

Natural or Manmade

Accidental or Intentional

Small or Large

Information Technology or Not

Cyber or Kinetic

- Fire
- Flooding
- IT failures
- Earthquakes
- Cyber attacks
- Severe weather
- Network failures
- Technology failures
- Organizational changes
- Loss of service provider
- Strikes or other labor actions
- Loss of customer or trading partner
- Chemical, biological, and nuclear hazards
- Unavailability of workforce
- Failed internal processes
- Supply chain disruption
- Employee kidnappings
- Workplace violence
- Data corruption
- Product failure
- Power outages
- Civil unrest
- Terrorism
- Fraud
- Etc.

Result in →

Interruption of Business Processes

…through which operational risks are realized

Yesterday vs. Today

Ever-Increasing Capability & Complexity
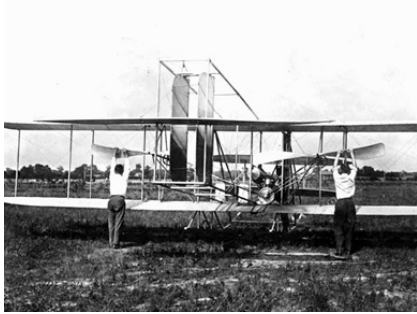
Biplane   **Apollo Lunar Module**   **SR-71**   **F-35**

0 SLOC   2K SLOC   500K SLOC   9.9M SLOC

SLOC = Source Lines of Code

Yesterday's mission success would have been…

Backup Tape

Application Software

Middleware

Database

Operating System

Iron Mountain Storage

LAN

WAN

Internet

Business Location

DR Site
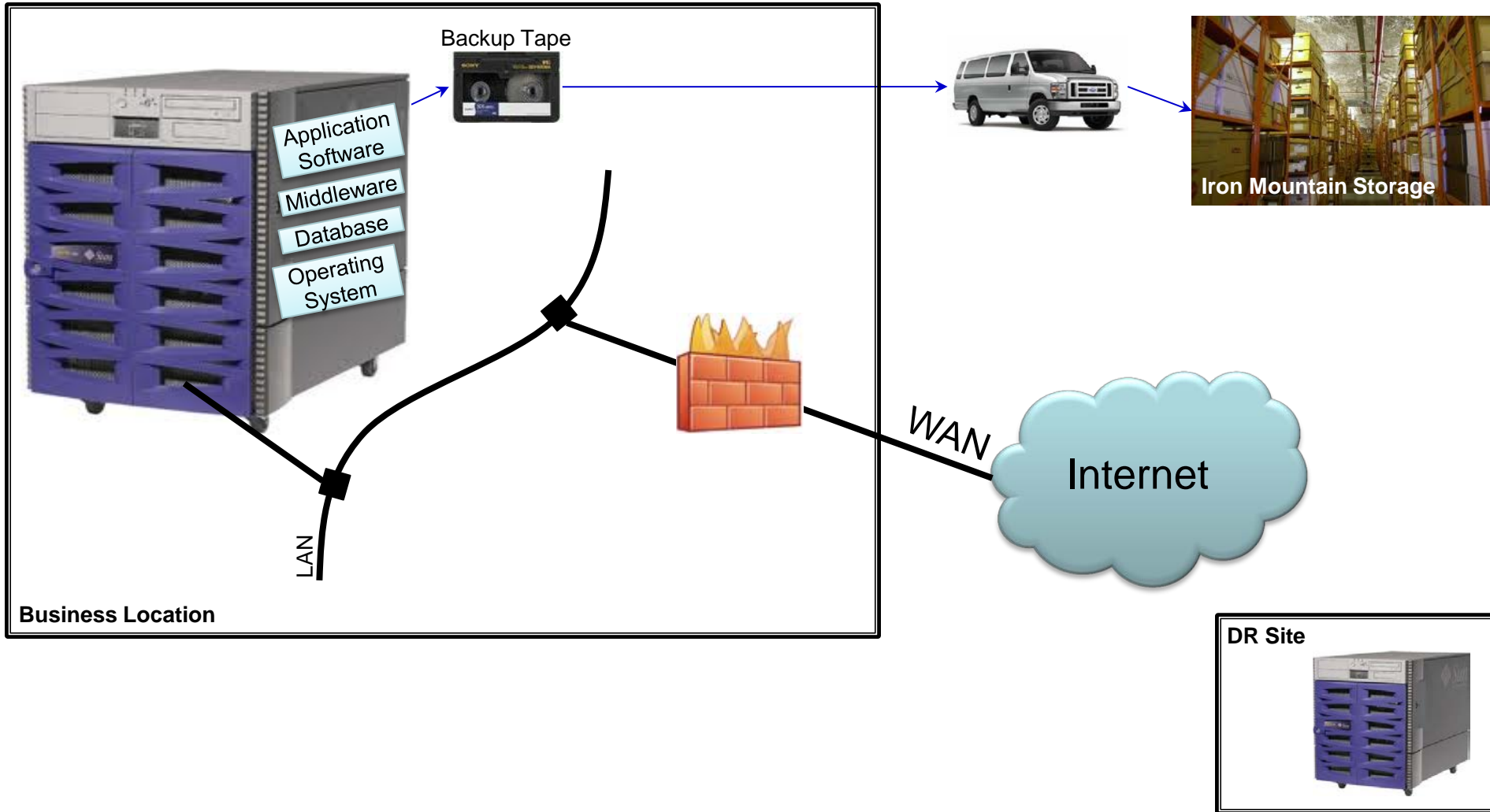
Today mission success is about …

Business process complexities

Application complexities
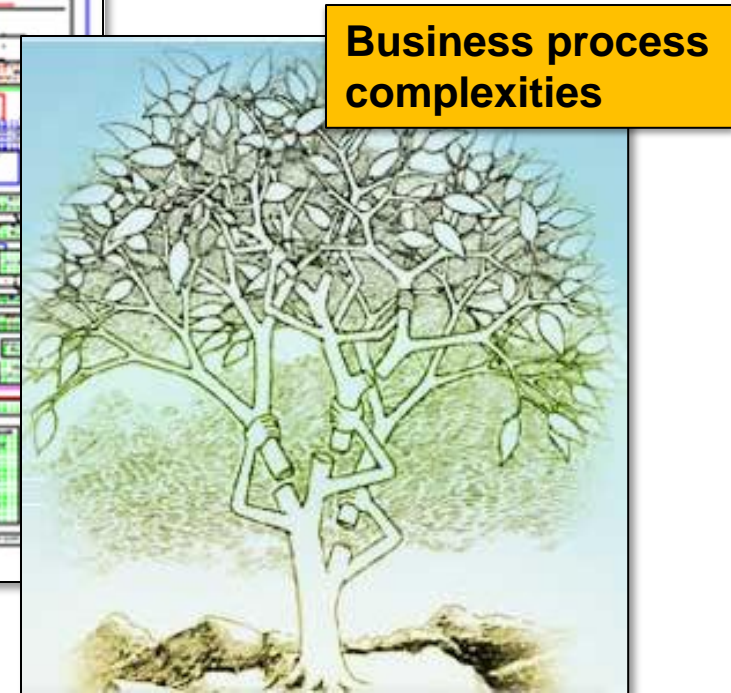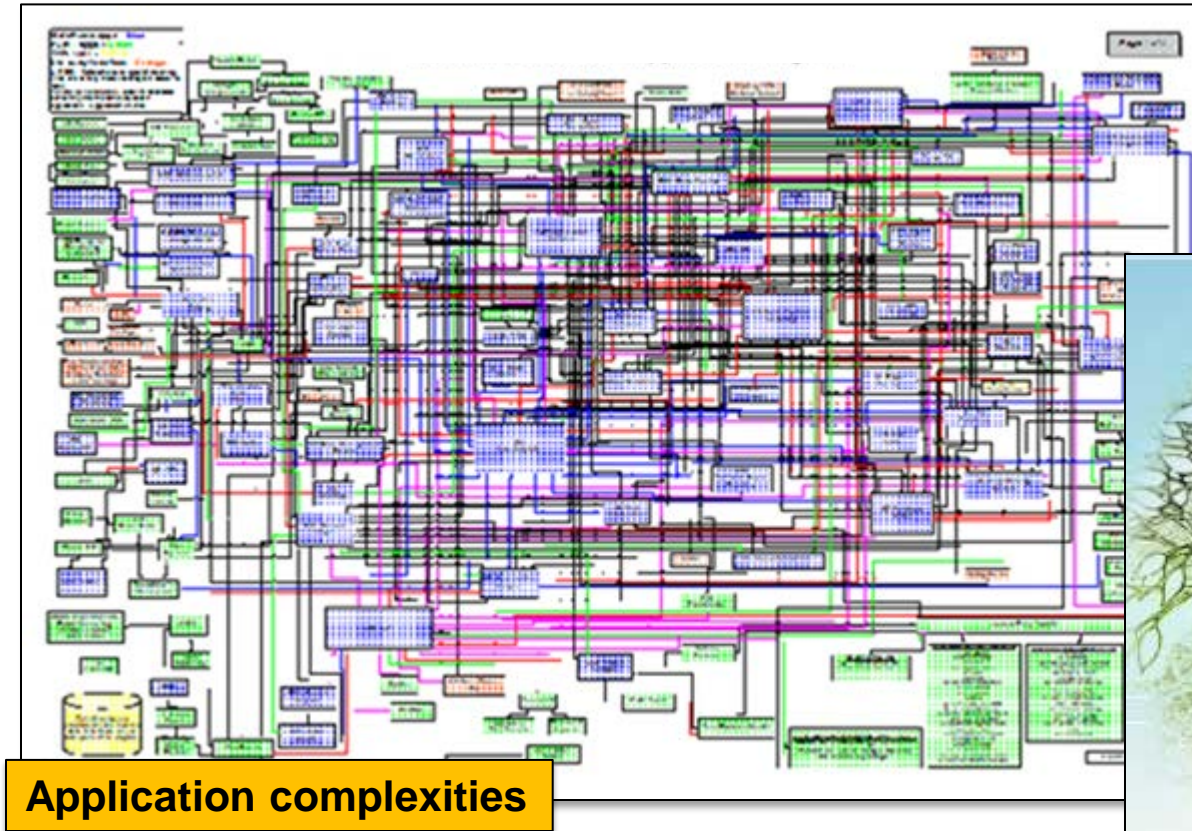
and more…

Yesterday's Mission Protection
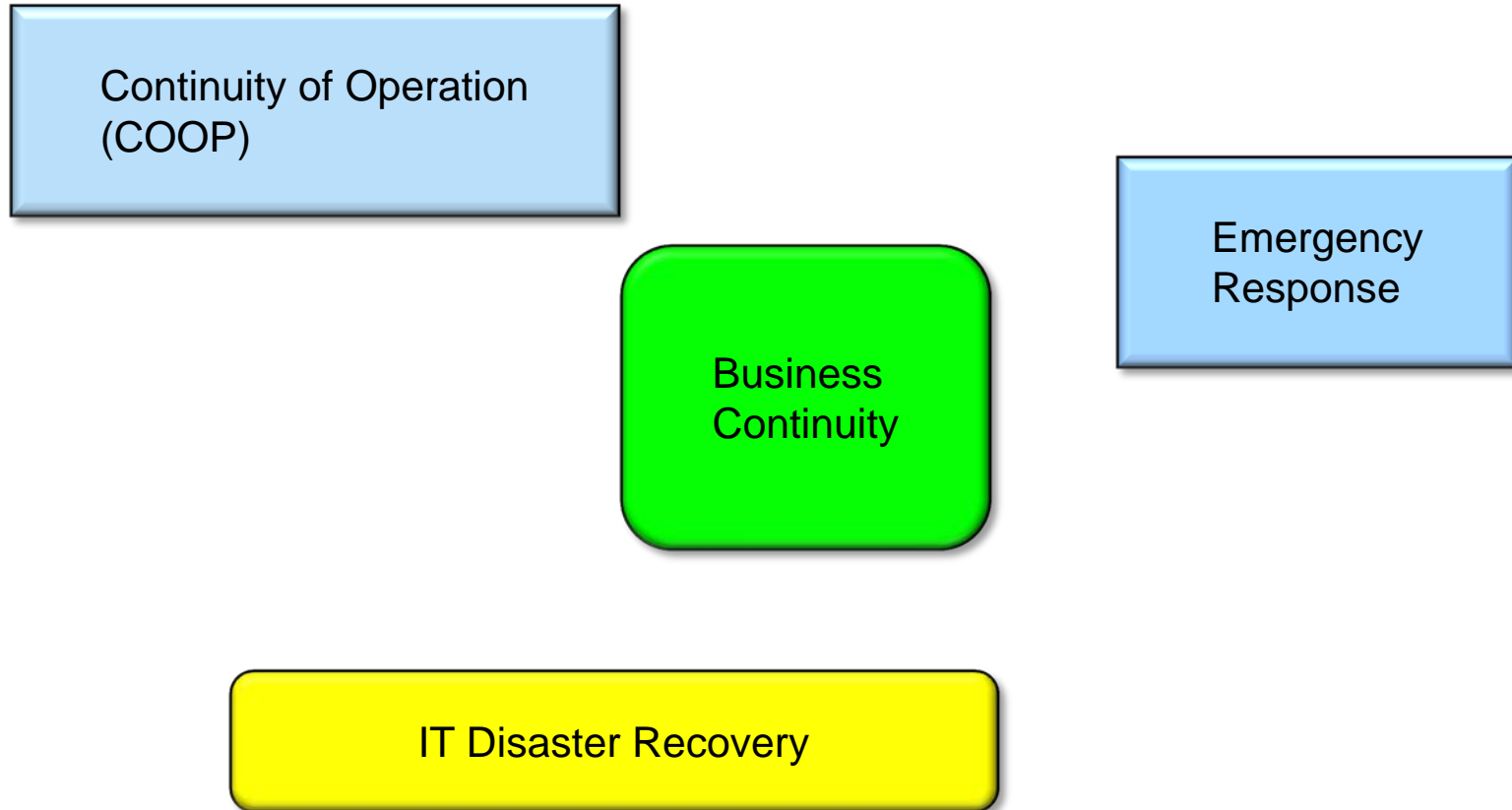
Continuity of Operation (COOP)

Emergency Response

Business Continuity

IT Disaster Recovery

Today's Mission Protection

Continuity of Operation (COOP)

Business Continuity

Crisis Communications

Contingency Planning

Emergency Management

Cyber Protection

Preparedness Planning

Crisis Management

Information Security

IT Operations

IT Disaster Recovery

Risk Management

Workforce Continuity

Supply Chain Continuity

Operational Risk Management

Pandemic Planning

Privacy

Enterprise Risk Management

Today's Business Environment
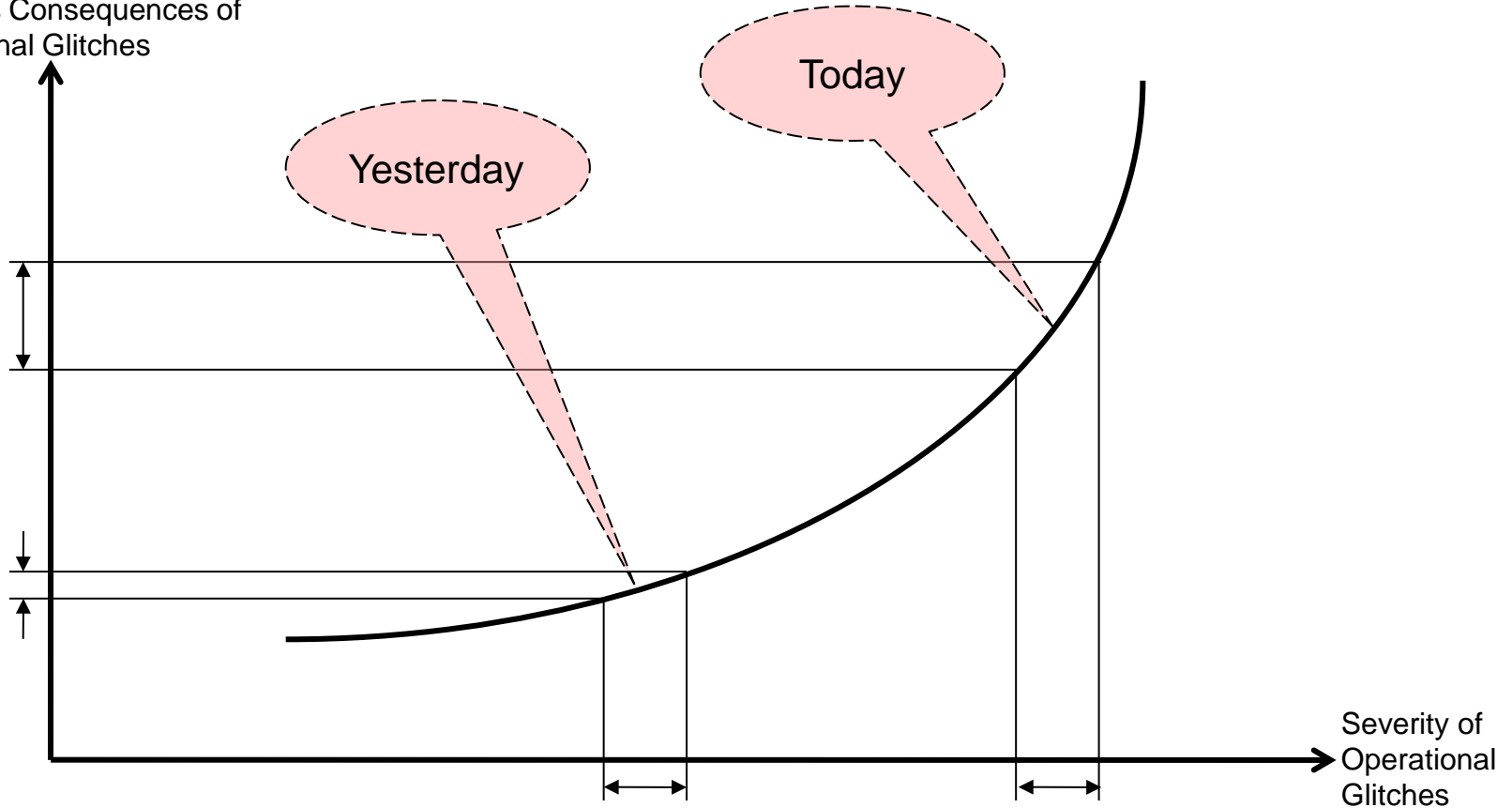
Today's Business Environment Is Much Less Forgiving

Operational Resilience

Operational Risk

A form of risk affecting day-to-day business operations

A very broad risk category
- from high-frequency low-impact to low-frequency high-impact

Exacerbated by
- actions of people
- systems and technology failures
- failed internal processes
- external events
- bad decisions

Enterprise Risk Management (ERM)

Operational Risk Management
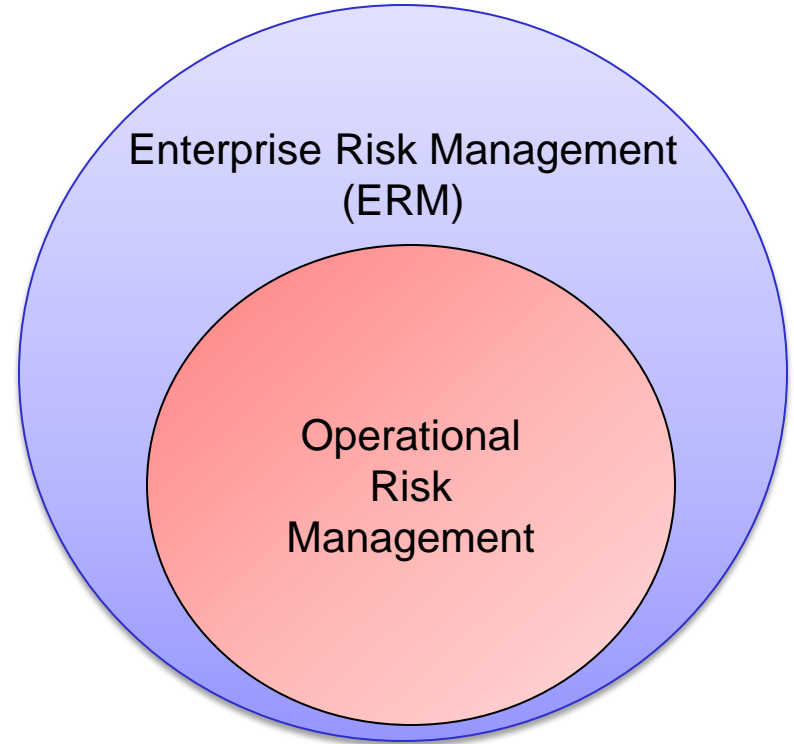
Why do operational risks matter?

Trust and confidence of employees and customers

Reputation and image

Regulatory compliance, fines, and legal penalties

Customer retention and growth

Life, safety, and health of customers and employees

Productivity and profitability

Organizational survival

… because they have explicit and direct IMPACT

re·sil·ience   *noun* [ri-ˈzil-yəns]

power or ability to return to the original form, position, etc. after being bent, compressed, or stretched

ability of an ecosystem to return to its original state after being disturbed

ability to recover from or adjust easily to misfortune or change

physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit

Resiliency

ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation

ability to recover readily from illness, depression, adversity, or the like

capability of a strained body to recover its size and shape after deformation

Operational Resilience

The **_emergent_** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated

Operational Resilience

The ***emergent*** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated

- Organization
- Nation
- Armed Forces
- Critical Infrastructure
- System
- Network
- Supply Chain
- Community
- An Ecosystem
- Cyberspace

An Analogy: Health

Is there a place that you can purchase health?

Is there a place where health is manufactured?

How do you become healthy?

Health & Resilience: They are both emergent properties.

Operational Resilience & Mission Success

To be operationally resilient, cyber- and/or kinetic-enabled missions must address operational risk on a number of "planes."
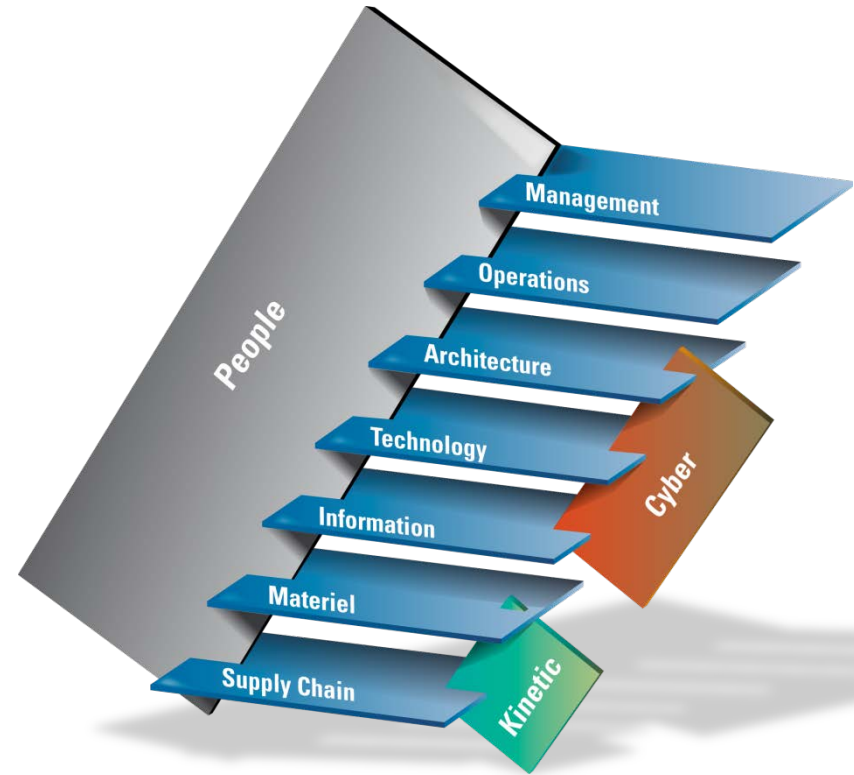
Operational Efforts Must Consider and Enable Such Multidimensionality

Organizational Mission - Revisited

Services and Products

Outputs of an organization

can be internally or externally focused.

Collectively they enable an organization's mission.

Example: U.S. Postal Service

Postage Stamps · Money Order · P. O. Box · International Mail · Domestic Mail Delivery · Certified Mail · Insured Mail · Registered Mail · Express Mail · Bulk Mail · USPS.com · Track Mail · Shipping Supplies · Passport Application · Hold Mail · Forward Mail · gopost · Election Mail · National Postal Museum · Postal Inspection Services · Critical Mail · Return Services · Philatelic Services · Etc.

Mission of USPS
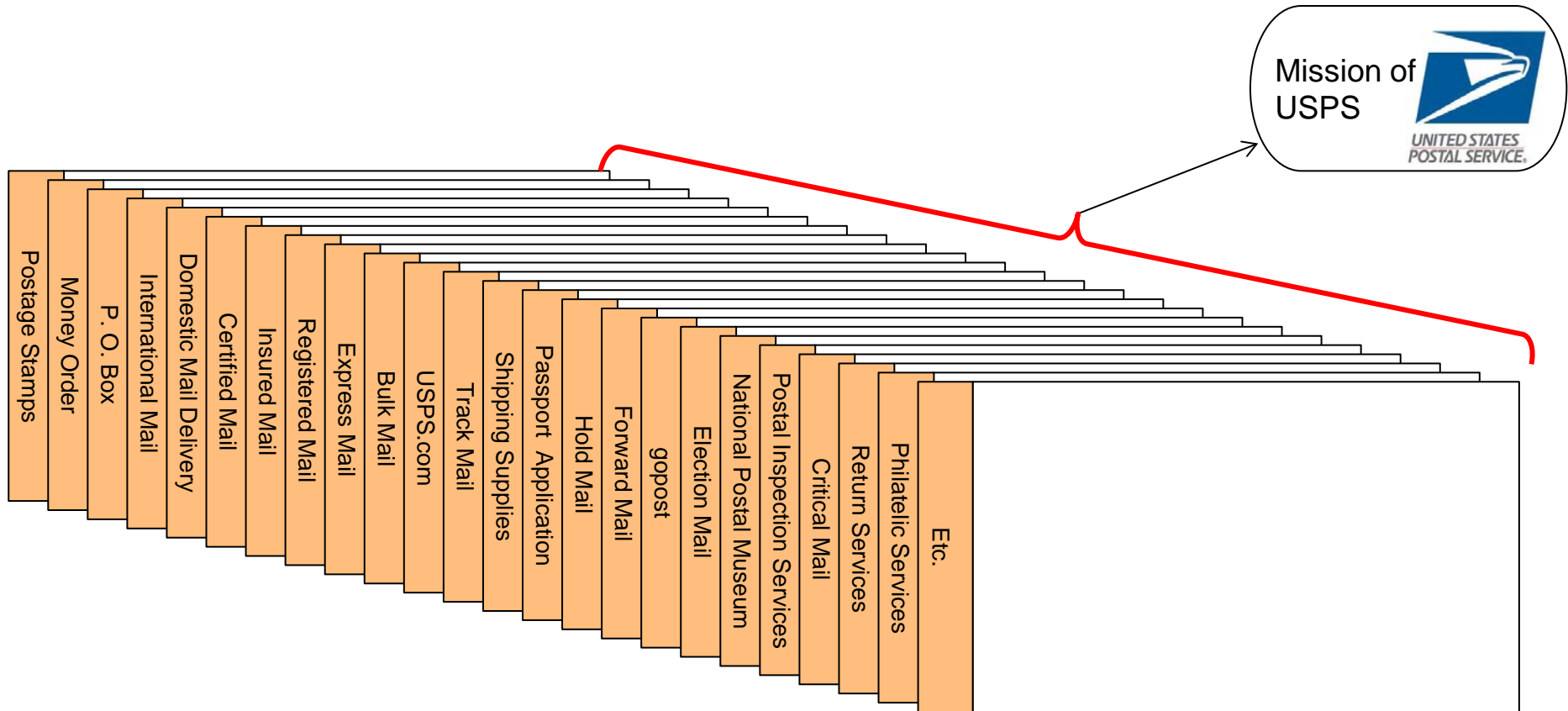
Productive Activities or Business Processes
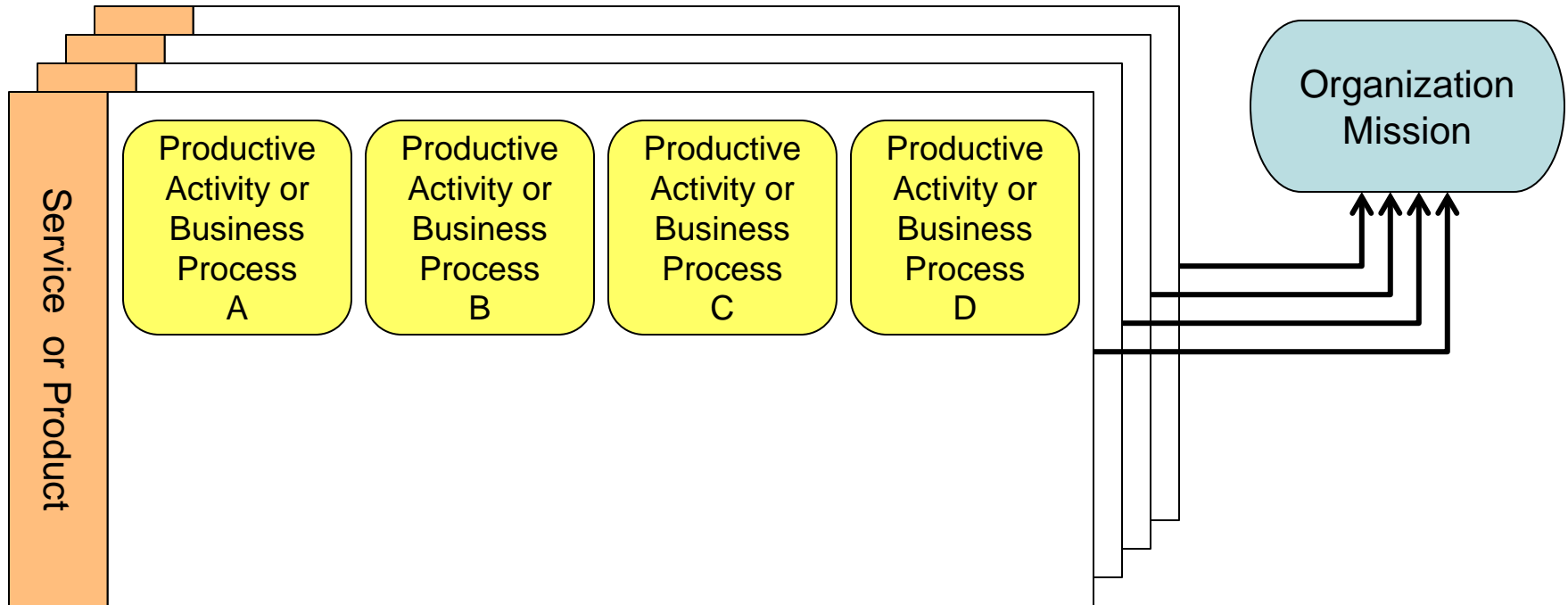
Activities that the organization (and/or its suppliers) perform to ensure that services and products are generated

A service or product is made up of one or more business processes.

Example: U.S. Postal Service
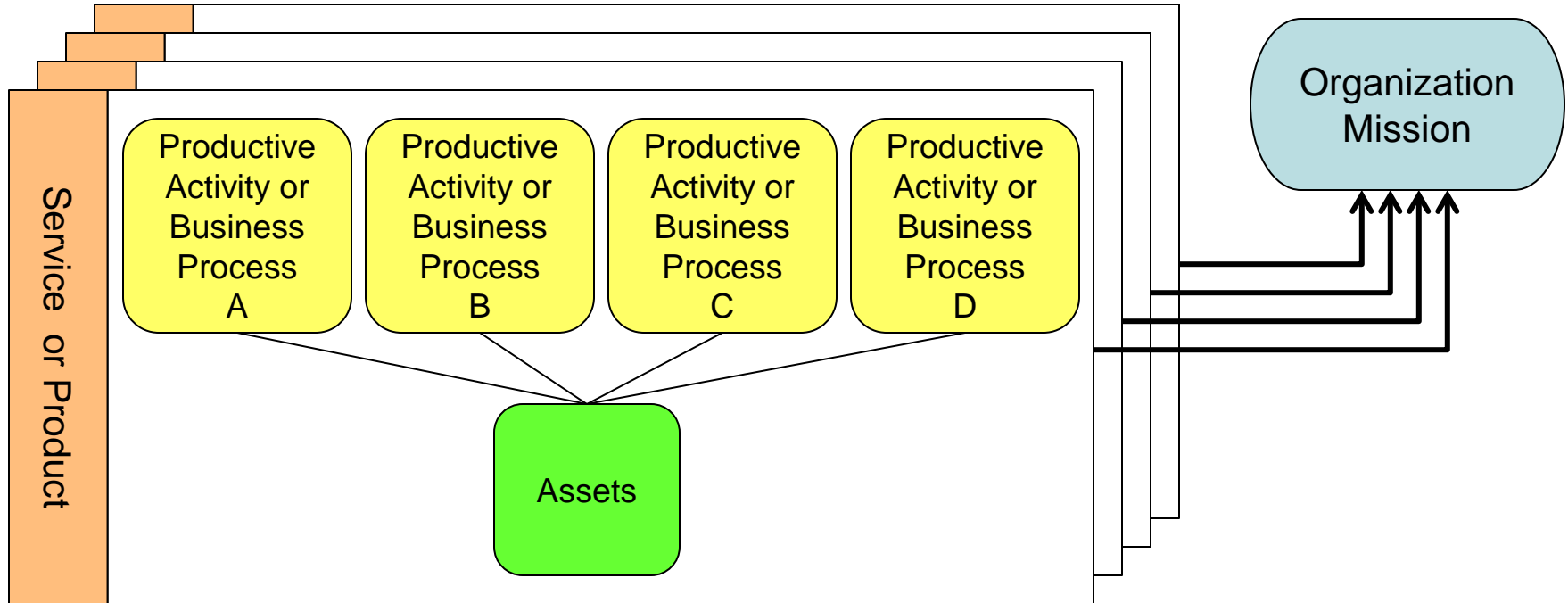
Domestic Mail Delivery	Payroll Services	IT Services	HR Services	Inspection Services	Software Development	Engineering	Mail Sorting	UPS & FedEx Services	Vehicle Fleet Services	Airline Services	Etc.

Assets

Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.

Asset Types of Importance to Operational Resilience

People

Information

Facilities

Technology

Supply Chain / Raw Material

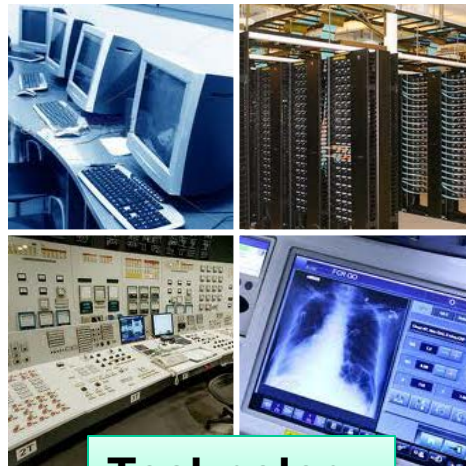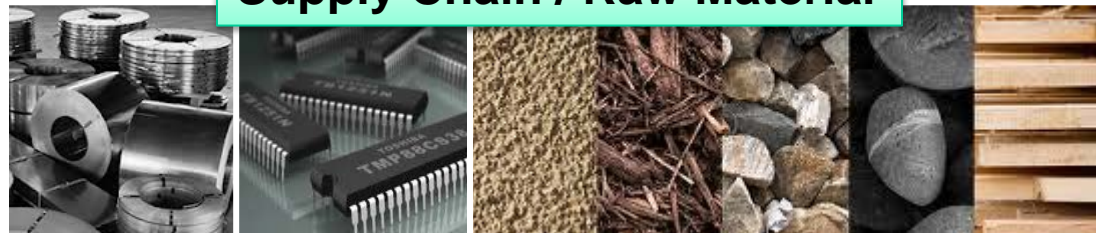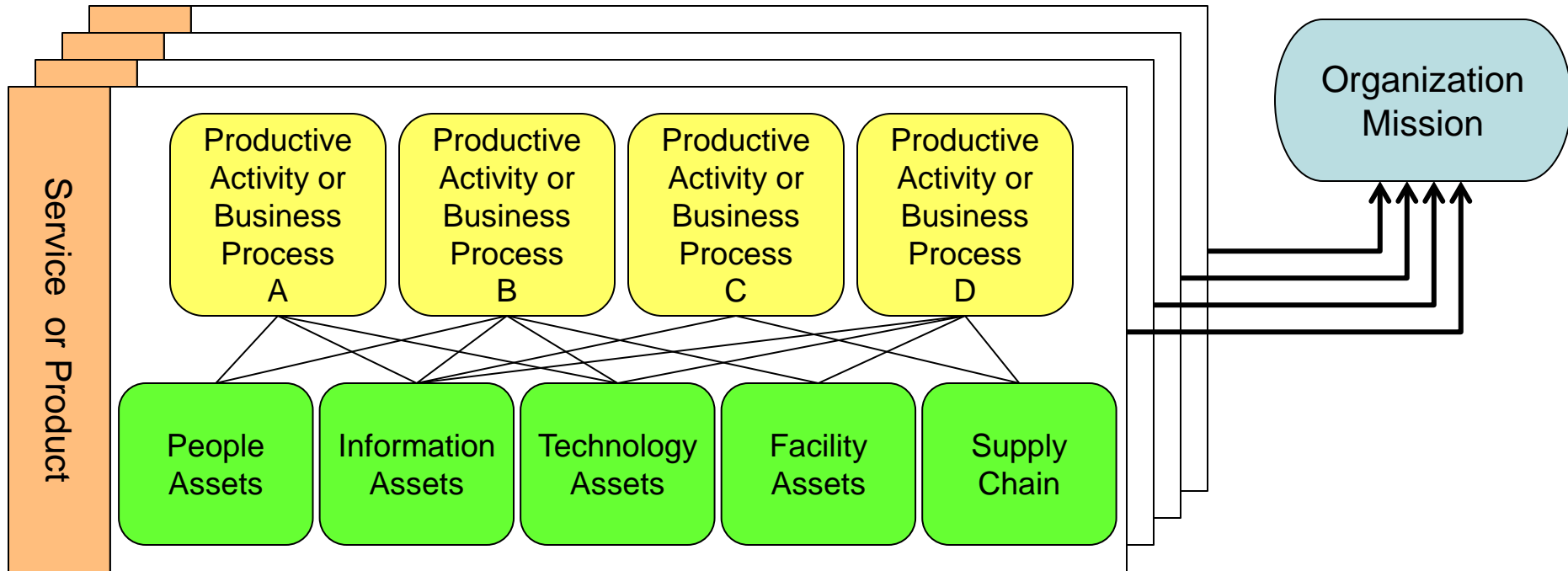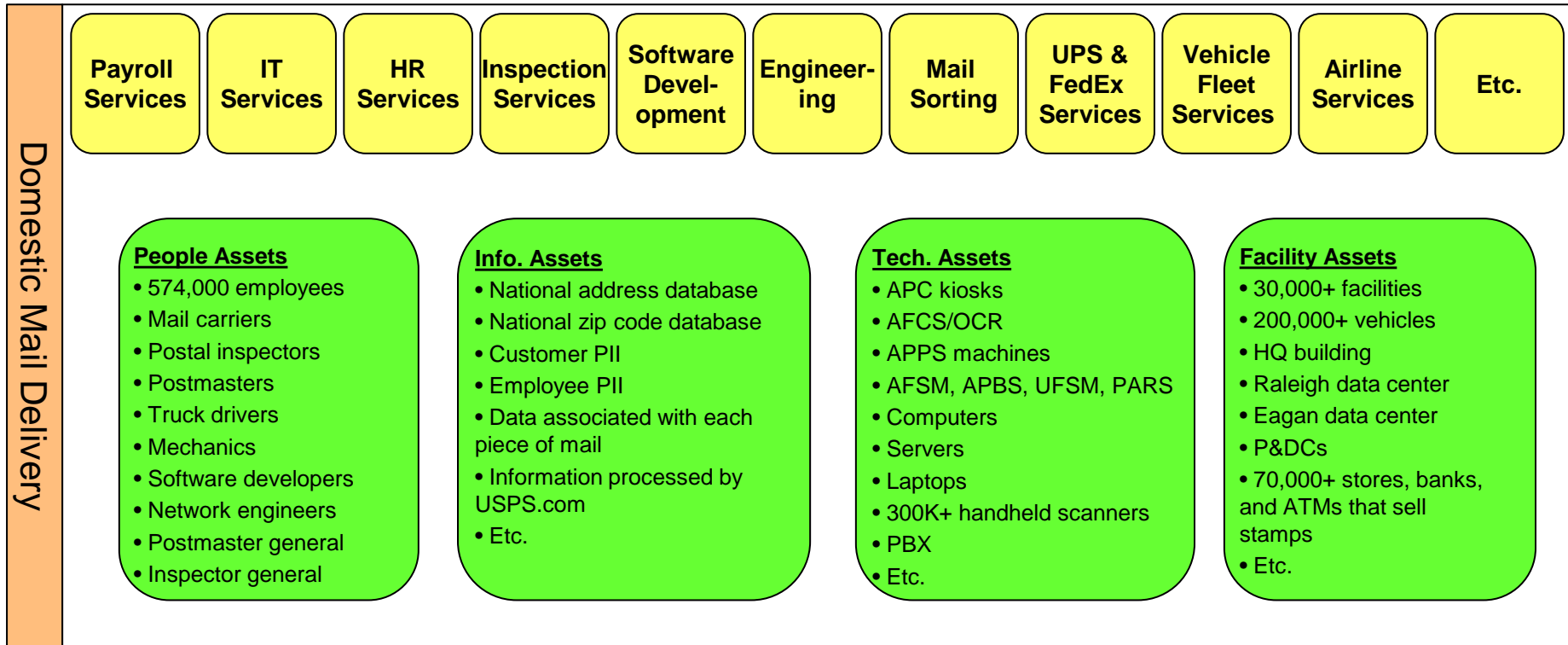CERT | Software Engineering Institute | Carnegie Mellon University
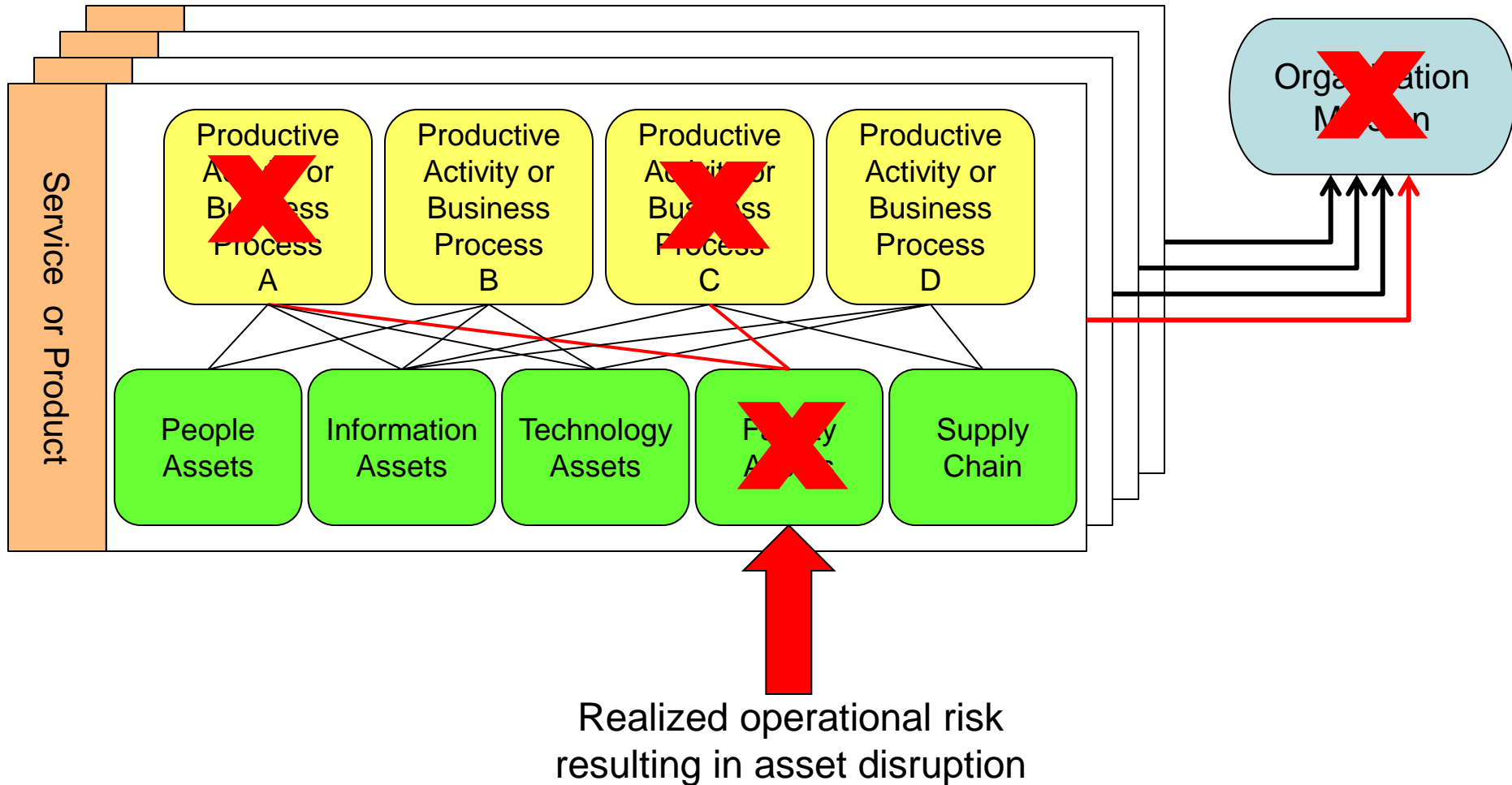
Asset Types

Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.

Example: U.S. Postal Service

| Domestic Mail Delivery | Payroll Services | IT Services | HR Services | Inspection Services | Software Devel-opment | Engineer-ing | Mail Sorting | UPS & FedEx Services | Vehicle Fleet Services | Airline Services | Etc. |

People Assets
- 574,000 employees
- Mail carriers
- Postal inspectors
- Postmasters
- Truck drivers
- Mechanics
- Software developers
- Network engineers
- Postmaster general
- Inspector general

Info. Assets
- National address database
- National zip code database
- Customer PII
- Employee PII
- Data associated with each piece of mail
- Information processed by USPS.com
- Etc.

Tech. Assets
- APC kiosks
- AFCS/OCR
- APPS machines
- AFSM, APBS, UFSM, PARS
- Computers
- Servers
- Laptops
- 300K+ handheld scanners
- PBX
- Etc.

Facility Assets
- 30,000+ facilities
- 200,000+ vehicles
- HQ building
- Raleigh data center
- Eagan data center
- P&DCs
- 70,000+ stores, banks, and ATMs that sell stamps
- Etc.

Operational Resilience Starts at Asset Level

Realized operational risk resulting in asset disruption

Operational Resilience Starts at Asset Level

Asset

Protect

Sustain

Event

Manage Conditions of Risk

Keep assets from exposure to disruption

(e.g., Fault-Tolerance & High-Availability Designs; Preparedness; Information Security)

Manage Consequences of Risk

Keep assets productive during adversity

(e.g., Disaster Recovery, Business Continuity, Pandemic Planning, Crisis Management, COOP)

Analogy - Protection and Sustainment Strategies

Protection Activities

- Translate into activities designed to keep assets from exposure to disruption

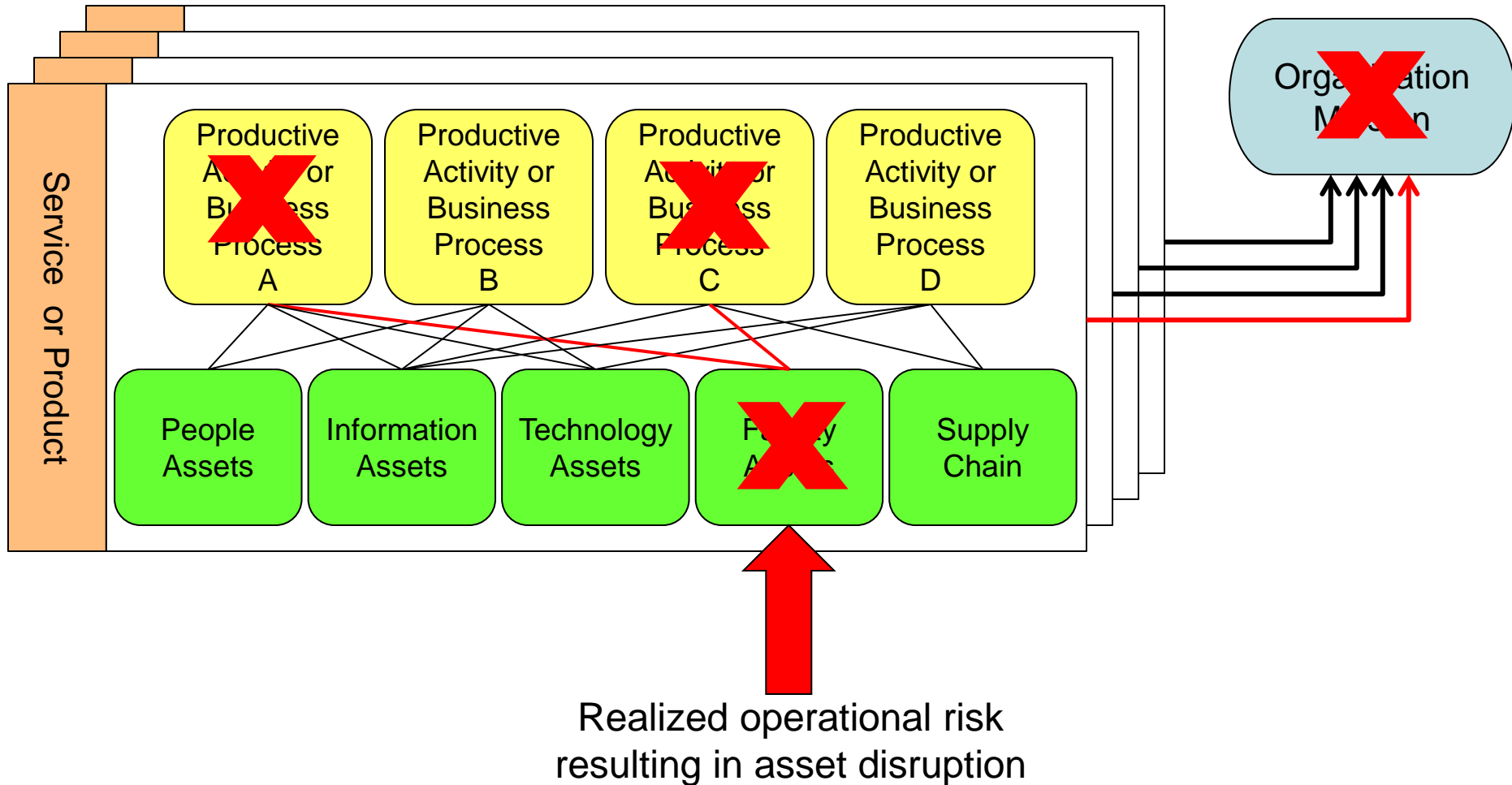- Example: "security" activities, but may also be embedded in IT operations activities
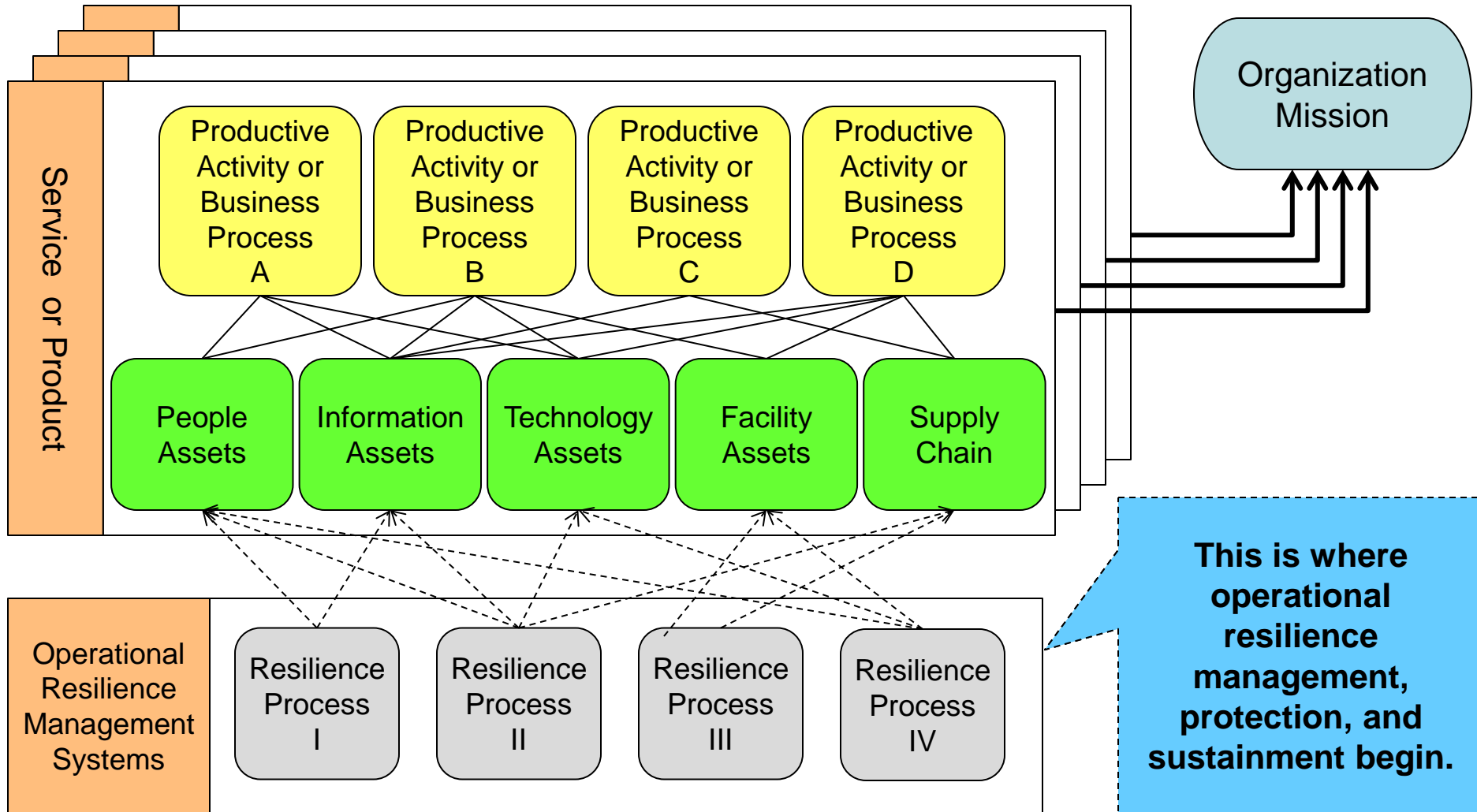

Sustainability Activities

- Translate into activities designed to keep assets productive during adversity

- Example: "business continuity" activities
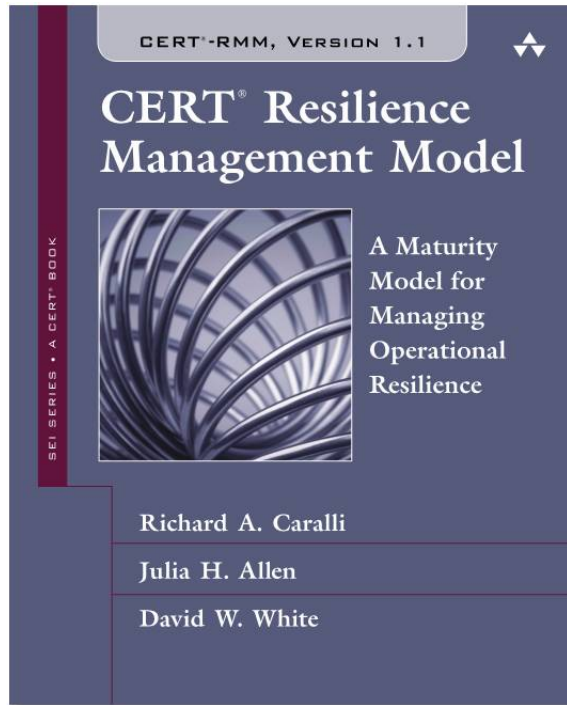
Asset Disruption

Realized operational risk resulting in asset disruption

Organizational Context for Resilience Activities

Service or Product

Productive Activity or Business Process A

Productive Activity or Business Process B

Productive Activity or Business Process C

Productive Activity or Business Process D

People Assets

Information Assets

Technology Assets

Facility Assets

Supply Chain

Organization Mission

Operational Resilience Management Systems

Resilience Process I

Resilience Process II

Resilience Process III

Resilience Process IV

This is where operational resilience management, protection, and sustainment begin.

CERT Resilience Management Model (CERT-RMM)

Framework for managing and improving operational resilience

http://www.cert.org/resilience/

"…an extensive super-set of the things an organization could do to be more resilient."

—CERT-RMM adopter

Desired Integrated Approach
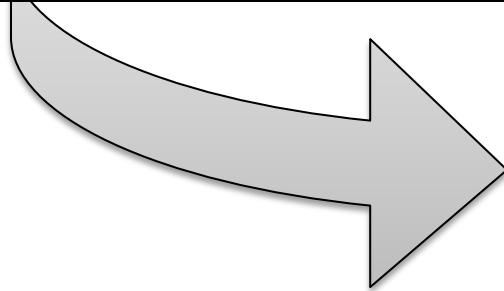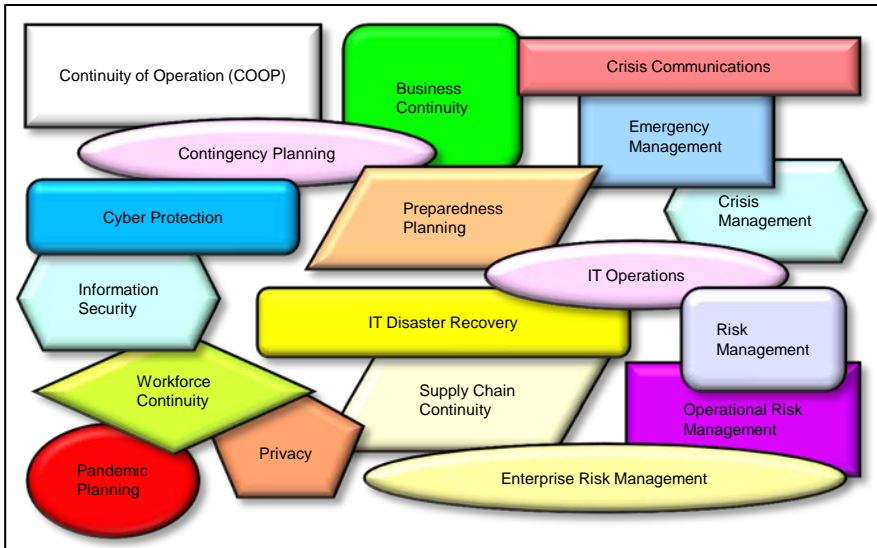
Pull for Integrated Cyber Resilience

Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements.

CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Federal Computer WEEK

Strategy and business management for government leaders

Updated homeland security strategy emphasizes resilience

Blueprint for a Secure Cyber Future

The Blueprint lists four goals for protecting critical information infrastructure:

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

Department of Defense
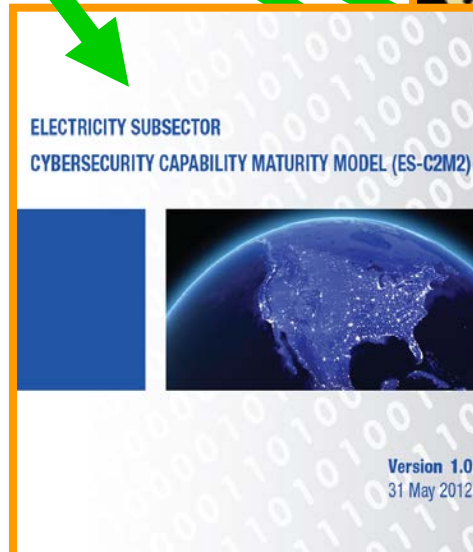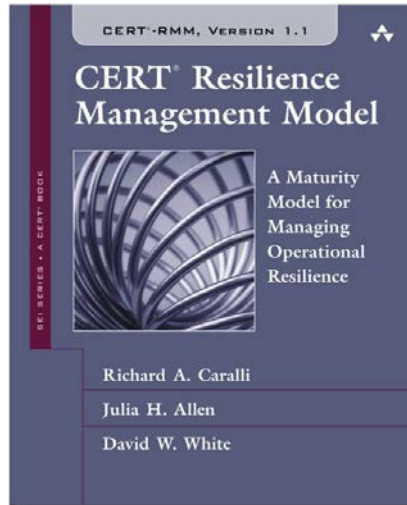
S&T Emphasis Areas

The Department has identified seven priorities:

- Defense Strategic Guidance
- Autonomy
- Counter Weapons of Mass Destruction
- Cyber Sciences
- Data-to-Decisions
- Electronic Warfare
- Engineered Resilient Systems
- Human Systems

Success Stories

A Sampling of CERT-RMM Applications and Derivatives

Department of Homeland Security

CYBER RESILIENCE REVIEW

U.S. DEPARTMENT OF HOMELAND SECURITY

The Cyber Security Evaluation Program (CSEP), within the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD), conducts a no-cost, voluntary Cyber Resilience Review (CRR) to evaluate and enhance cyber security capacities and capabilities within all 18 Critical Infrastructure and Key Resources (CIKR) Sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments. The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization.

Overview

The CRR is based on the CERT Resilience Management Model (CERT-RMM) developed by Carnegie Mellon University's Software Engineering Institute [www.cert.org/resilience/rmm.html]. The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services and assets during normal operations and during times of operational stress and crises.

The CRR seeks to elicit the current state of cyber security management practices from key cyber security personnel—Chief Information Officers, Chief Information Security Officers, and those responsible for management of IT Security, IT Operations, and Business Continuity.

The CRR results in a report that summarizes observed strengths and weaknesses in each domain and provides options for consideration containing general guidance or activities aimed at improving the cyber security posture and preparedness of an organization.

CRR Domains & Asset Types

The CRR focuses on the following ten domains:
1. Asset Management
2. Configuration and Change Management
3. Risk Management
4. Controls Management
5. Vulnerability Management
6. Incident Management
7. Service Continuity Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The CRR addresses the following four asset types:
1. People
2. Information
3. Technology
4. Facilities

What to Expect
- The CRR is a one-day, on-site facilitation and interview of key cyber security personnel.
- The participants will receive a draft report within 45 calendar days to review and provide feedback report results. DHS will subsequently issue a final CRR Report.
- CRR results are afforded protections under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/PCII]— the results are for organization use and DHS does not share results.

Contact Information for CRR-related Inquiries
Please address inquiries regarding the CRR to: CSE@hq.dhs.gov (Cyber Security Evaluations).

About DHS and NCSD

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. NCSD leads DHS's efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.

ES-C2M2

ELECTRICITY SUBSECTOR

CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0
31 May 2012

U.S. Postal Inspection Service (USPIS)

The law enforcement arm of the U.S. Postal Service

The USPIS has used CERT-RMM to address such operational risks as

- export screening

- new product security

- measuring and monitoring risks associated with fraud

- physical security and aviation screening for international mail

- improved processes for investigative response to network security incidents

Lockheed Martin

Library

Seminal works and reference material created by SEI staff.

Search the Library   Browse by Topic   Browse by Type

Application of the CERT® Resilience Management Model at Lockheed Martin

Lockheed Martin Corporation has collaborated with the Software Engineering Institute on the application of the CERT Resilience Management Model (CERT-RMM) to improve Lockheed Martin's corporate-wide business continuity, IT disaster recovery, crisis management, and pandemic planning activities. Two CERT-RMM Class C appraisals have been conducted as part of the collaboration. This presentation will provide an overview of the project, information about the appraisals, and a summary of the use of the appraisal results.

LOCKHEED MARTIN

In Closing

Hurricane Sandy Surprised Us in Many Ways

Devastating Fire

Run on Power Strips

Blizzard

Sandstorm

Most Talked-About Subject Afterward…

Cornell University

CHRONICLE ONLINE

March 4, 2013

Arctic ice loss amplified Superstorm Sandy violence

By Blaine Friedlander

If you believe that last October's Superstorm Sandy was a freak of nature -- the confluence of unusual meteorological, atmospheric and celestial events -- think again.

Cornell and Rutgers researchers report in the March...

Bloomberg Businessweek
Politics & Policy

Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Life

It's Global Warming, Stupid

By Paul M. Barrett on November 01, 2012 | 1282 Comments

Yes, yes, it's unsophisticated to blame any given storm on climate change. Men and women in white lab coats tell us—and they're right—that many factors contribute to each severe weather episode. Climate deniers exploit scientific...

CLIMATEPROGRESS

How Does Climate Change Make Superstorms Like Sandy More Destructive?

By Joe Romm on Oct 31, 2012 at 5:03 pm

The New York Times
Tuesday, March 19, 2013

Environment

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | S

A Blog About Energy and the Environment

SCIENCE | October 30, 2012, 5:46 pm | 178 Comments

Did Global Warming Contribute to Hurricane Sandy's Devastation?

By JUSTIN GILLIS

Hurricane Sandy Damage Partly Caused By Climate Change, Scientists Say

Posted: 11/06/2012 10:06 am EST Updated: 11/06/2012 10:06 am EST

Most Talked-About Subject Afterward…

Is this the most important question to ask?

A better question to ask: *How has the national risk environment changed?*

Movement from traditional wireline telephony to cell phones and broadband cable telephony

Cutting The Lifeline
The percentage of cellphone-only households is growing

40% ········· July – Dec. 2011: **34%**

30

20

10

0

2008 '09 '10 '11

Source: CDC/NCHS surveys of 136,228 households conducted Jan. 2008–Dec 2011; 95% confidence interval
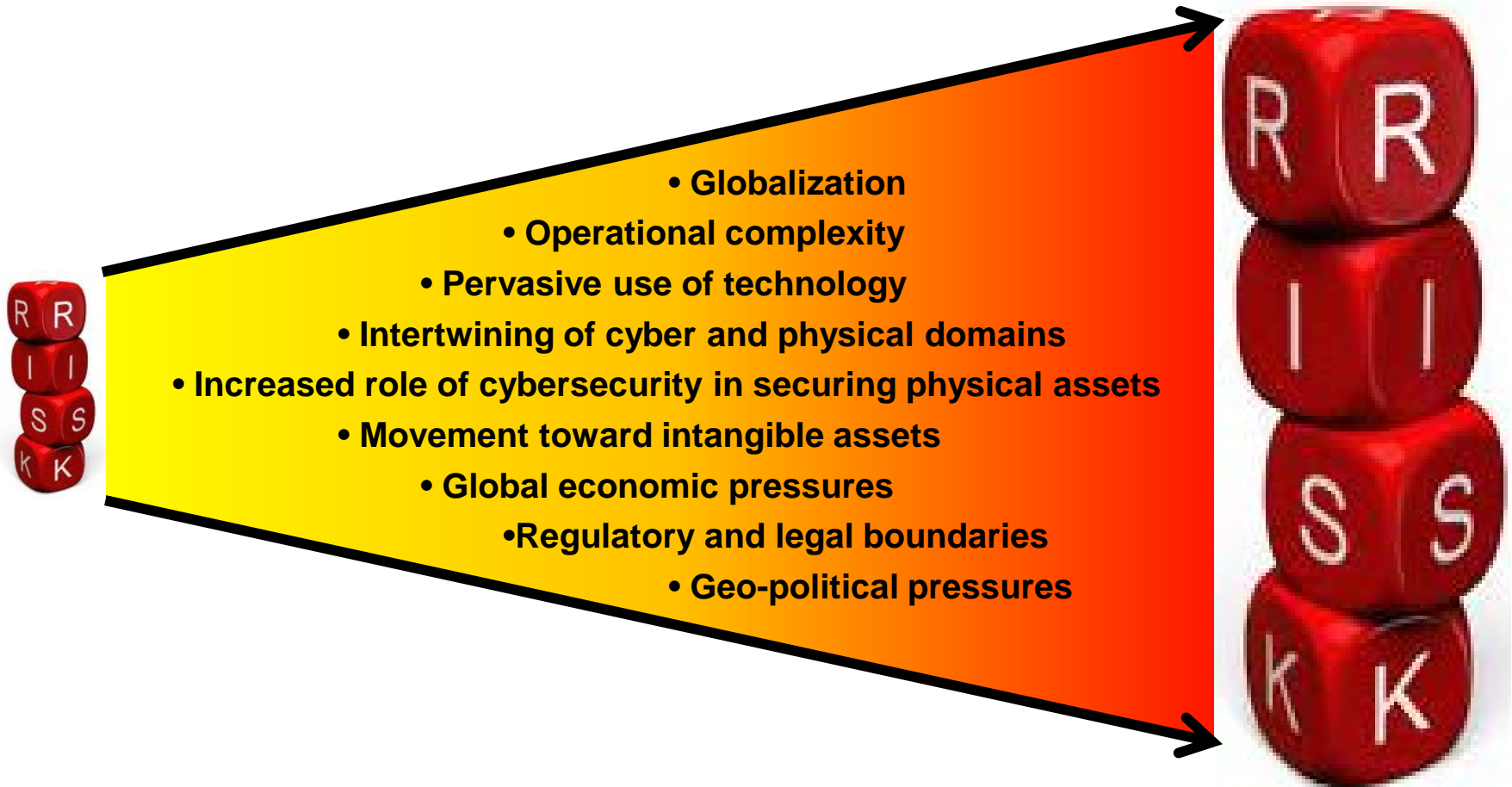The Wall Street Journal

Dependency on large number of mobile devices needing frequent recharging

"… As of 2003, 153 million Americans lived in coastal counties – an increase of 33 million since 1980 – and 3.7 million lived within a few feet of high tide…"

—*Bryan Walsh, Time Magazine, November 12, 2012*

… and there are many more.

Expansion of National Risk Environment

- Globalization
- Operational complexity
- Pervasive use of technology
- Intertwining of cyber and physical domains
- Increased role of cybersecurity in securing physical assets
- Movement toward intangible assets
- Global economic pressures
- Regulatory and legal boundaries
- Geo-political pressures

Successful management of operational risk may require a (significant) shift in thinking and approach.

Protecting the enterprise remains a complex and multifaceted challenge.

Disruptive events, through which risks are realized, will continue to surprise us.

Traditional tools, techniques, and methods may not work as well in this environment.

How should an enterprise deal with (and plan for) such surprises?

How should an enterprise operate in such an environment?

Promising Approaches

Next generation of integrated cyber-resilience management frameworks?

MODELS

Resilience Engineering – A new engineering discipline?

EDUCATION

RISK MGMT

Re-shaping (not fighting with) the risk landscape?

Should organizations be legally allowed to fight back when under cyber attack?

POLICY

Mechanisms to compose resilient systems from brittle components?

TECHNOLOGY

> "The oak fought the wind and was broken,
> the willow bent when it must and survived."
>
> *Robert Jordan, The Fires of Heaven*

Thank you for your attention…